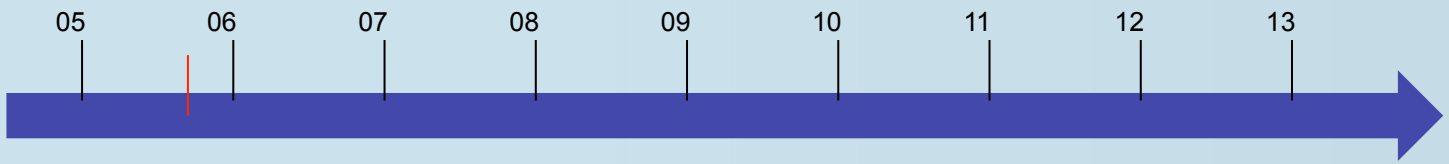
KATHOLIEKE UNIVERSITEIT
LEUVEN

The SHA-3 Process

Keccak & SHA-3 day
Brussels, 27 March 2013

Timeline



Summer 2005: Attacks on MD5, RIPEMD, SHA-0, SHA-1

The Wang effect

Before 2005

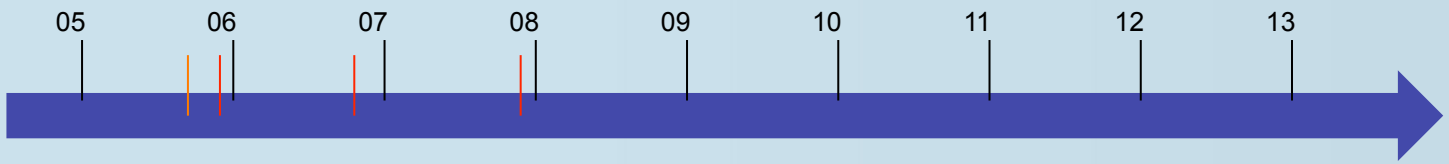
- MD4 (Dobbertin)
- MD5 (Boss., Den Boer)
- SHA (Chabaud-Joux)
- SHA-1
- SHA-2

After Wang

- MD4 (seconds)
- MD5 (hours)
- SHA (days)
- SHA-1 (months (?))
- SHA-2 (?)

We need a competition like for the AES!

Timeline



Nov 2005: 1st NIST workshop

Aug 2006: 2nd NIST workshop

Nov 2007: Start of the competition

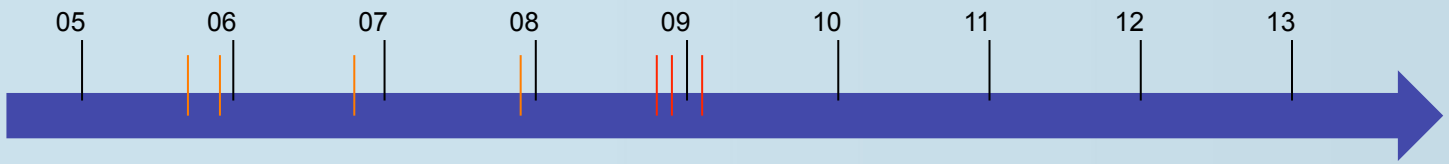
NIST call: requirements

- To support 3 digest lengths: 256, 384, 512
- Should work with HMAC
- Resistance against collision, preimage attacks, …
  - Length extension attacks, …

- “Look” random
- Sufficiently different from SHA-2

- Let the games begin …

Timeline

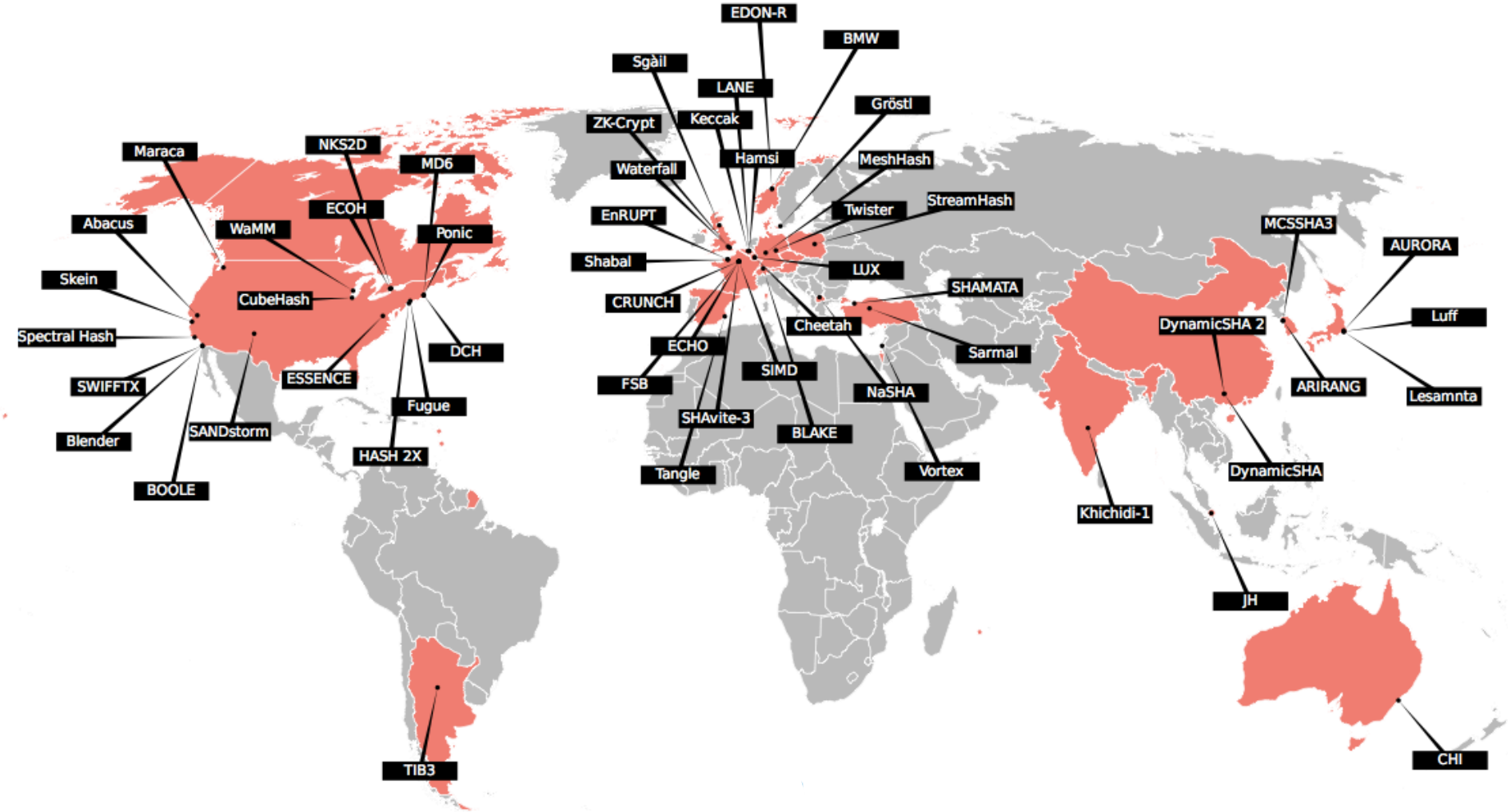


Oct 2008: End of submission (64)

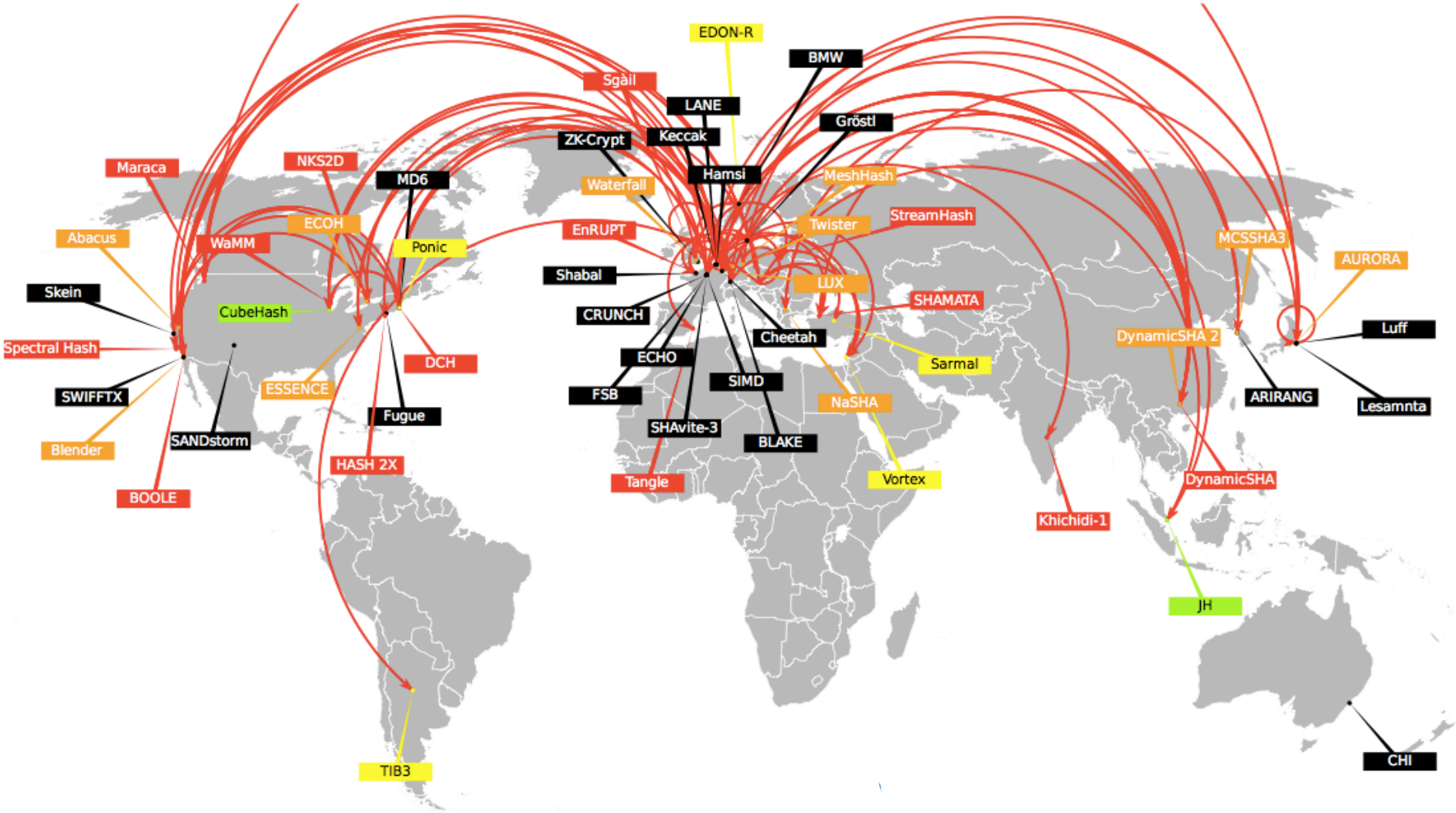
Dec 2008: Start of round 1 (51)

Feb 2009: 1st SHA-3 candidate conference

Submissions



The battlefield



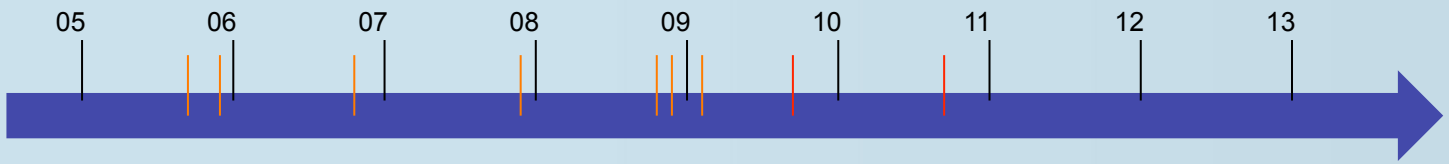
Round 1 victims (+ Round 0)

Abacus	Neil Sholer	2nd-preimage
ARIRANG	Jongin Lim	
AURORA	Masahiro Fujita	2nd preimage
Blender	Colin Bradbury	collision, preimage
Boole	Greg Rose	collision
Cheetah	Dmitry Khovratovich	
CHI	Phillip Hawkes	
CRUNCH	Jacques Patarin	
DCH	David A. Wilson	collision
Dynamic SHA	Xu Zijie	collision
Dynamic SHA2	Xu Zijie	collision
ECOH	Daniel R. L. Brown	2nd preimage
Edon-R	Danilo Gligoroski	preimage
EnRUPT	Sean O'Neil	collision
ESSENCE	Jason Worth Martin	collision
FSB	Matthieu Finiasz	
HASH 2X	Jason Lee	2nd-preimage
Khichidi-1	M. Vidyasagar	collision
LANE	Sebastiaan Indesteege	
Lesamnta	Hirotaka Yoshida	
LUX	Ivica Nikolić	collision, 2nd preimage

Maraca	Robert J. Jenkins	preimage
MCSSHA-3	Mikhail Maslennikov	2nd preimage
MD6	Ronald L. Rivest	
MeshHash	Björn Fay	2nd preimage
NaSHA	Smile Markovski	collision
NKS2D	Geoffrey Park	collision
Ponic	Peter Schmidt-Nielsen	2nd-preimage
SANDstorm	Rich Schroeppel	
Sarmal	Kerem Varıcı	preimage
Sgàil	Peter Maxwell	collision
SHAMATA	Orhun Kara	collision
Spectral Hash	Çetin Kaya Koç	collision
StreamHash	Michal Trojnara	collision
SWIFFTX	Daniele Micciancio	
Tangle	Rafael Alvarez	collision
TIB3	Daniel Penazzi	collision
Twister	Michael Gorski	preimage
Vortex	Michael Kounavis	preimage
WaMM	John Washburn	collision
Waterfall	Bob Hattersley	collision
ZK-Crypt	Carmi Gressel	

ehash.iaik.tugraz.at/wiki/The **SHA-3 Zoo**

Timeline



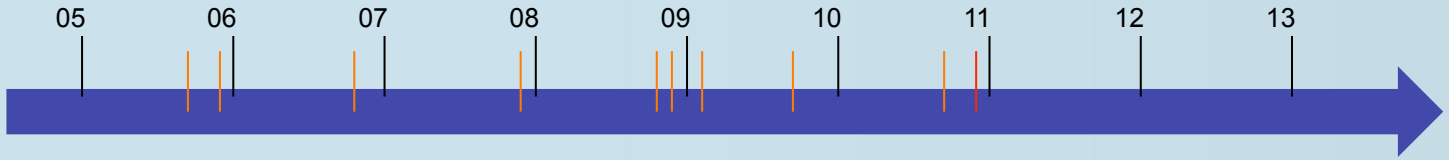
July 2009: Start of round 2 (14)

Aug 2010: 2nd SHA-3 candidate conference

Round 2 victims

Blue Midnight Wish	Svein Johan Knapskog	
CubeHash	Daniel J. Bernstein	preimage
ECHO	Henri Gilbert	
Fugue	Charanjit S. Jutla	
Hamsi	Özgül Küçük	
Luffa	Dai Watanabe	
Shabal	Jean-François Misarsky	
SHAvite-3	Orr Dunkelman	
SIMD	Gaëtan Leurent	

Timeline



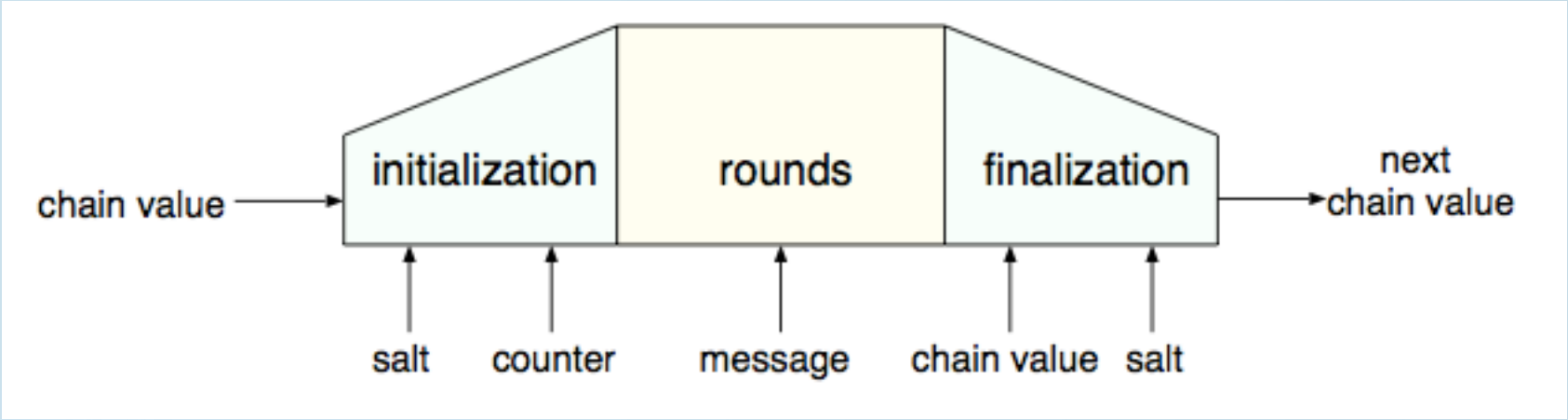
Dec 2010: Start of round 3 (5)

The 5 finalists

- Blake
  - JP Aumasson, L Henzen, W Meier, RCW Phan
- Grøstl
  - P Gauravaram, LR Knudsen, K Matusiewicz, F Mendel, C Rechberger, M Schläffer, SS Thomsen
- JH
  - H Wu
- Keccak
  - G Bertoni, J Daemen, M Peeters, G Van Assche
- Skein
  - N Ferguson, S Lucks, B Schneier, D Whiting, M Bellare, T Kohno, J Callas, J Walker

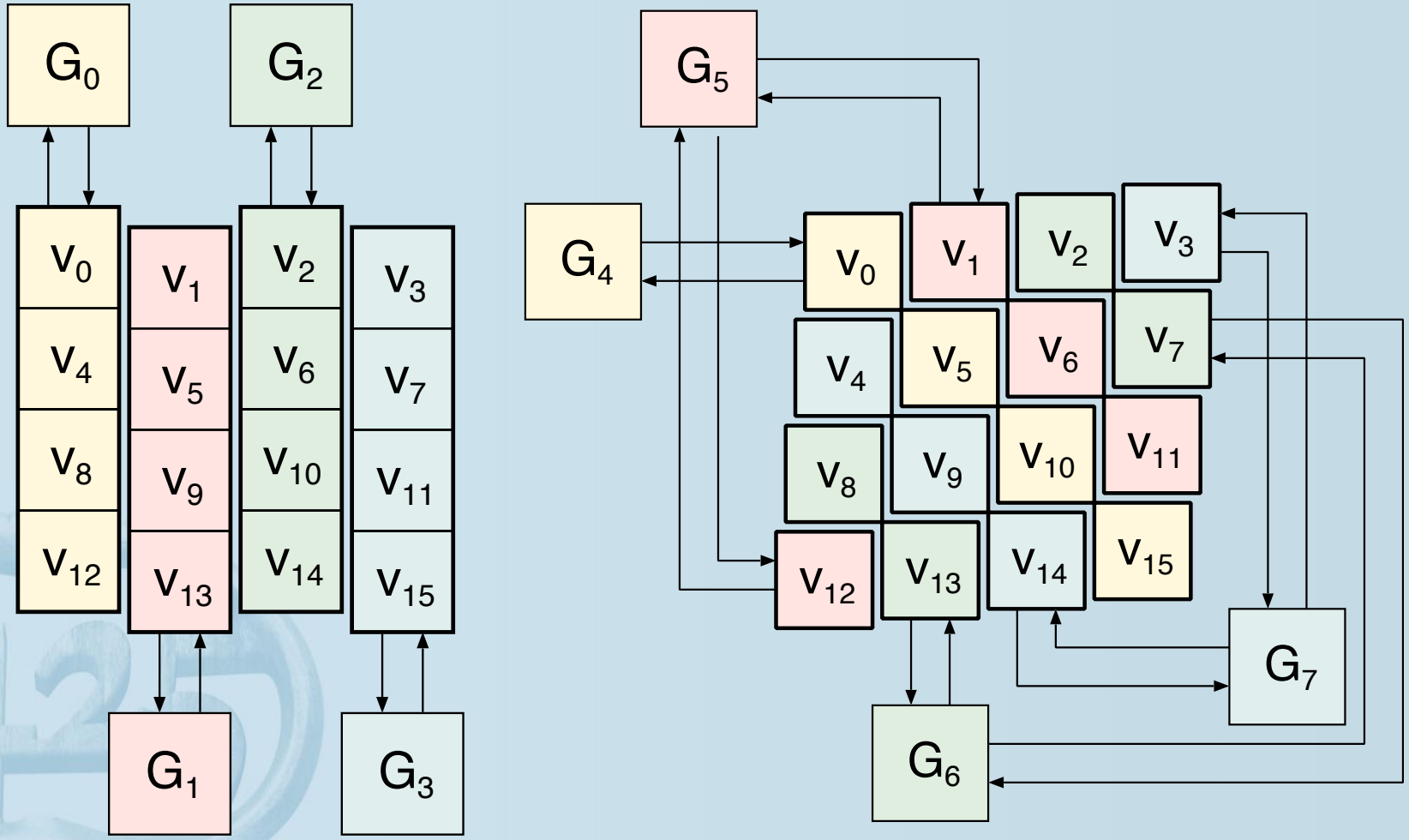
Blake

- Local wide-pipe

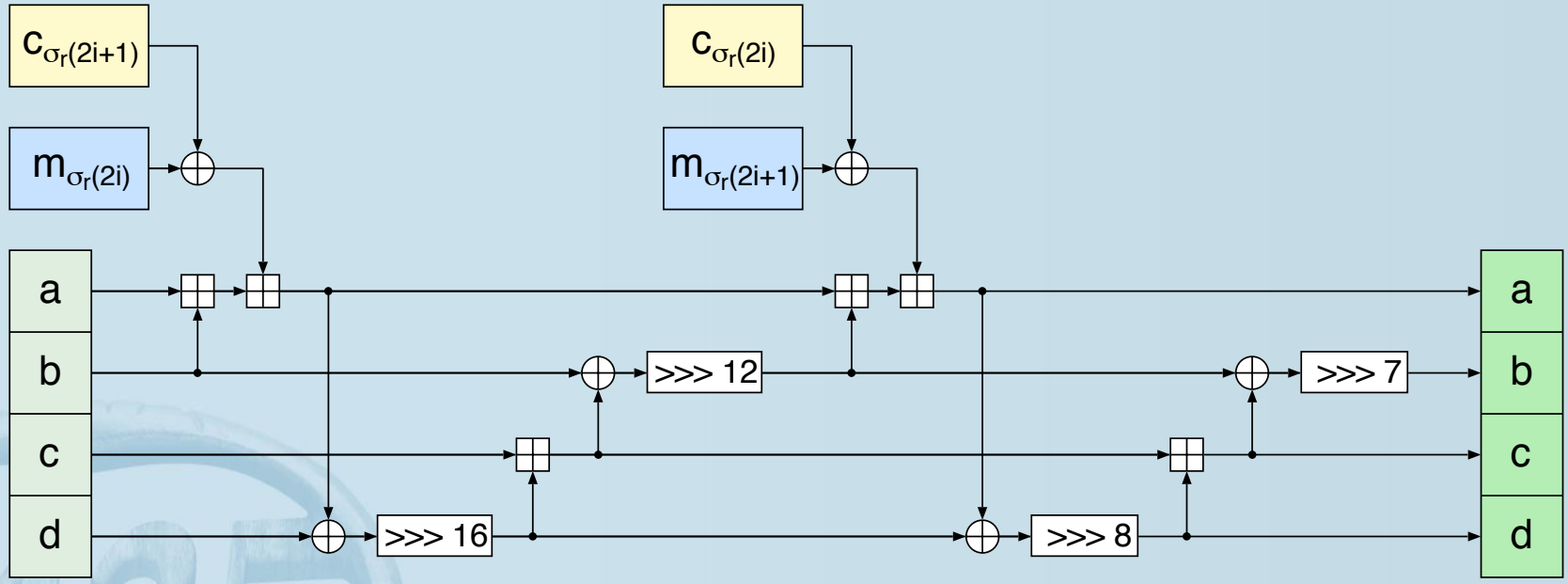


- Round function inspired by Salsa, Chacha
- 14/16 rounds

Blake


G0
G2
G5
G4
v0
v1
v2
v3
v4
v5
v6
v7
v8
v9
v10
v11
v12
v13
v14
v15
G1
G3
G6
G7

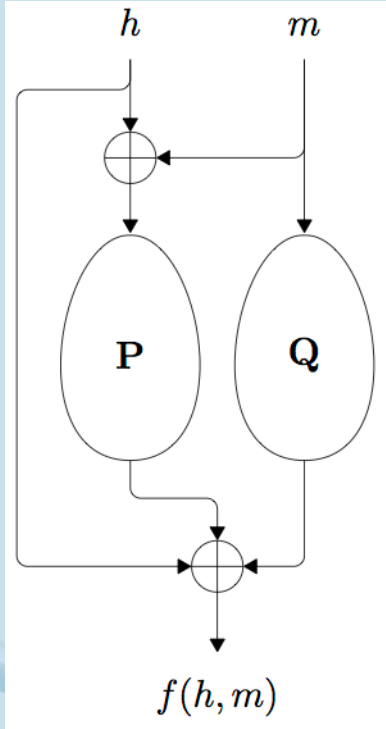
Blake G-function (1/8-round)

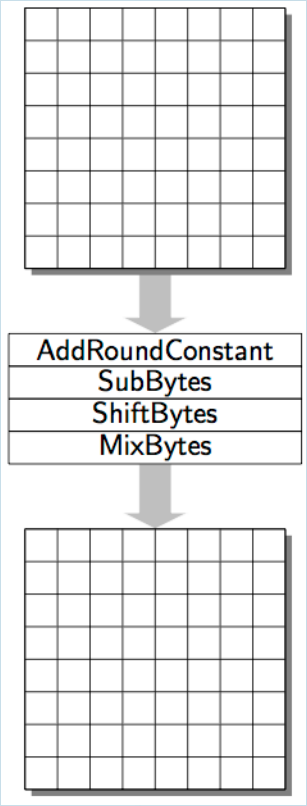


Blake features

- ARX
- Many rounds *and* fast
- Learned from mistakes in Lake

Grøstl

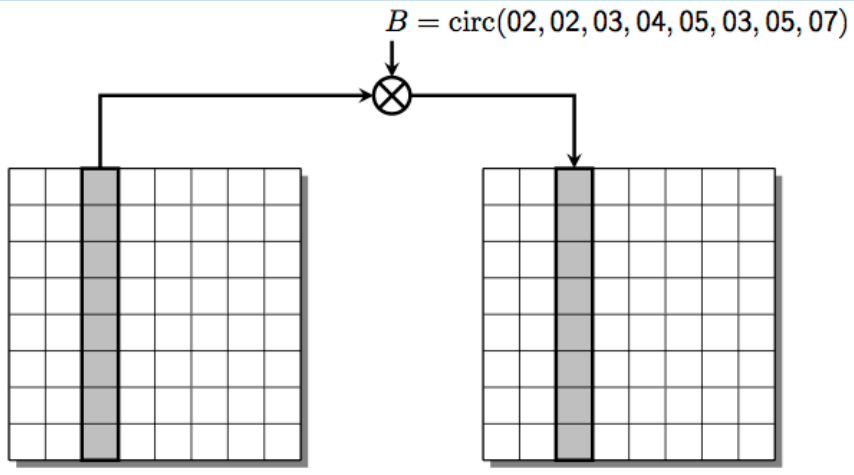




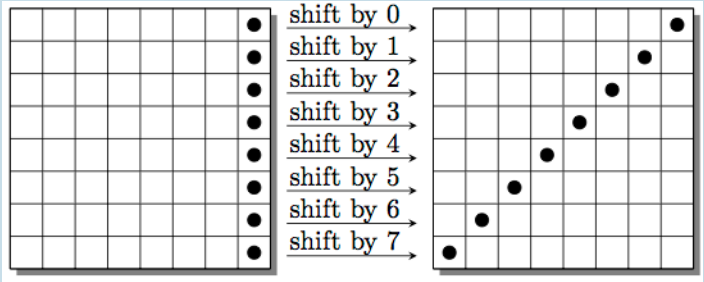
- 10/14 rounds

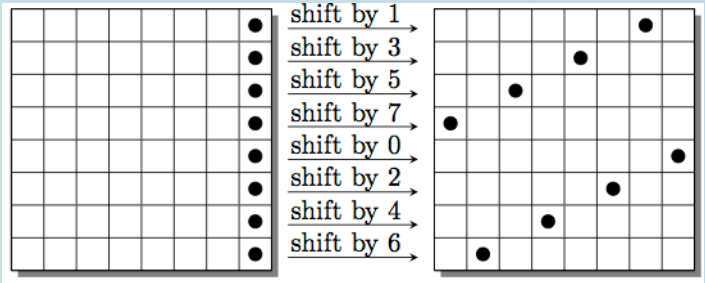
“AESsy” operations

MixBytes

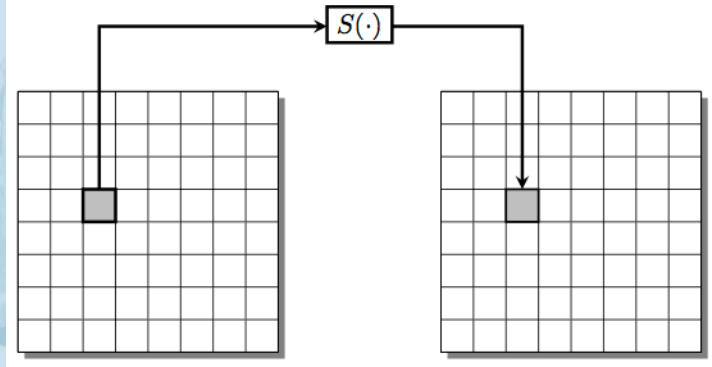


ShiftBytes





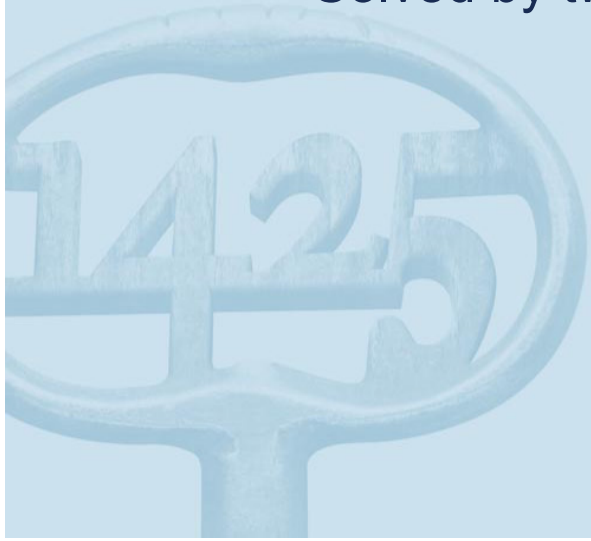
SubBytes



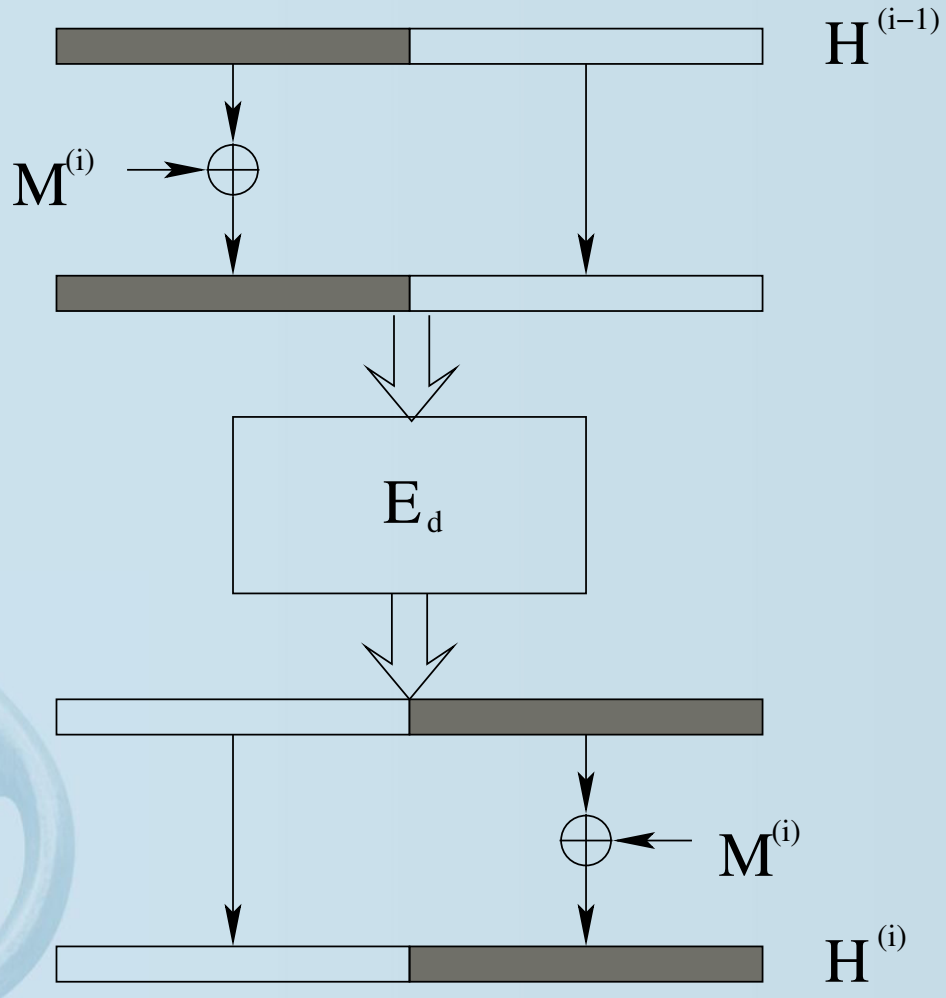
Grøstl features

- Substitution-Permutation Network
- Fast when AES instructions available
- Permutation-based design

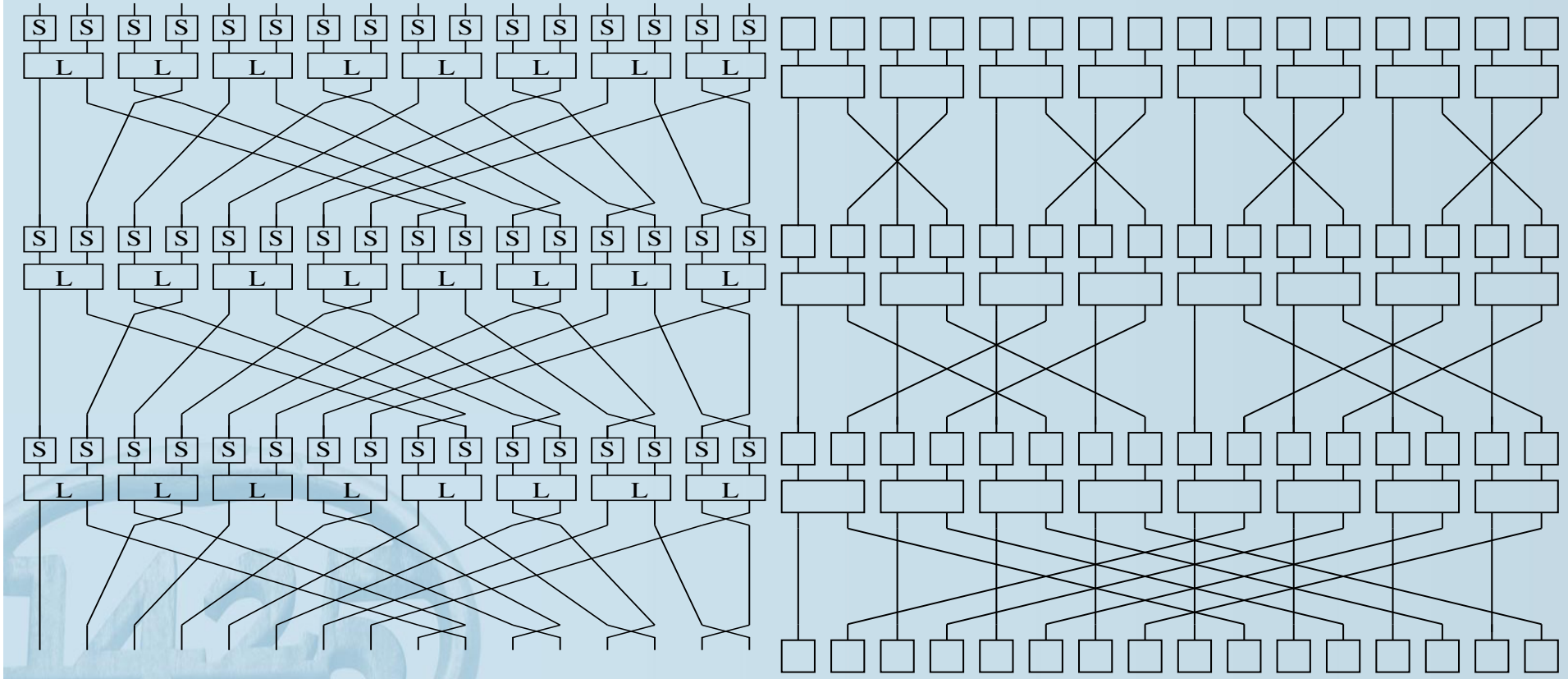
- Problem with “internal differential” attack
  - Solved by tweak



JH

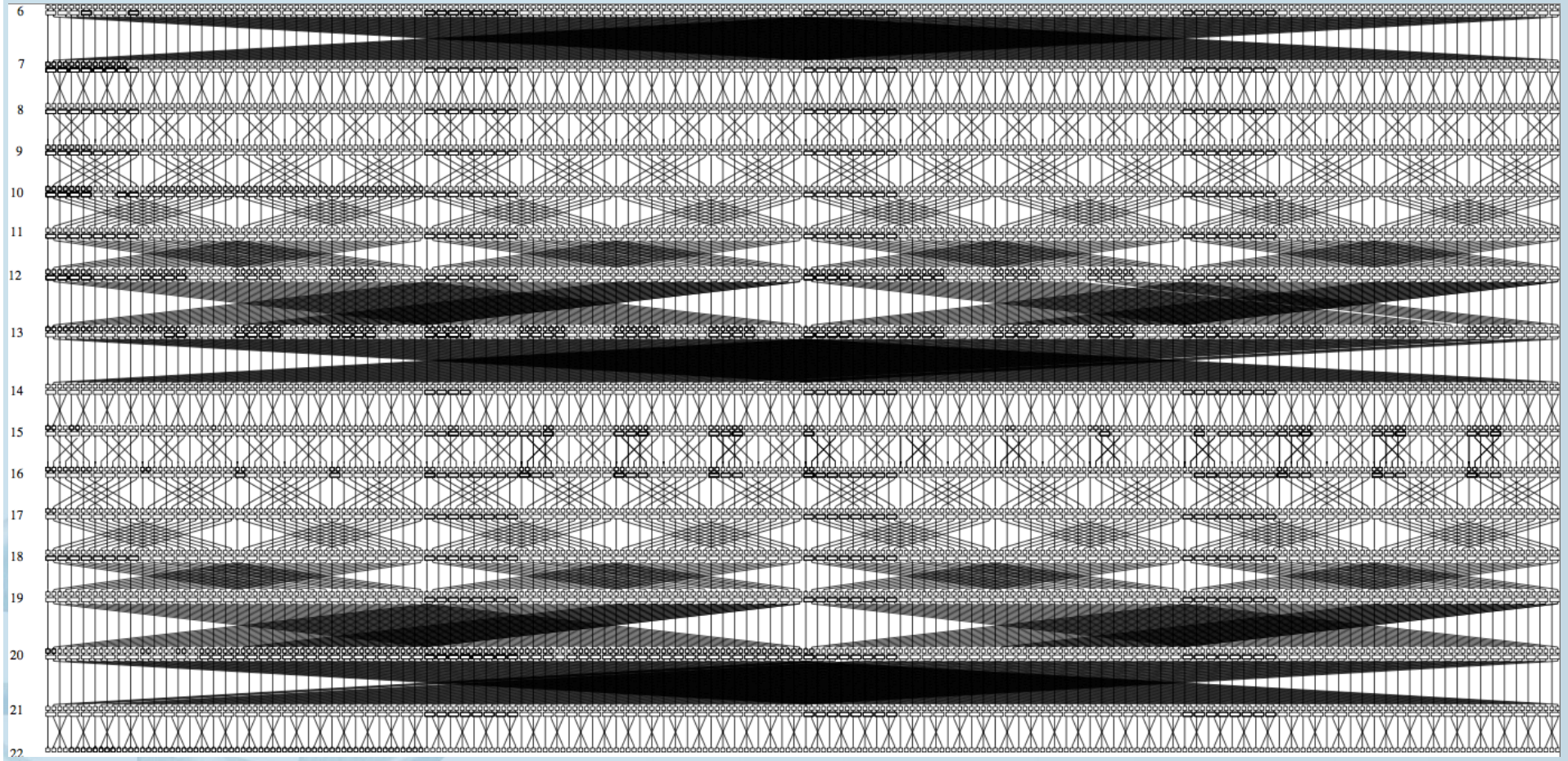


JH



- 4-bit S-boxes (2)
- 2-input MDS layer

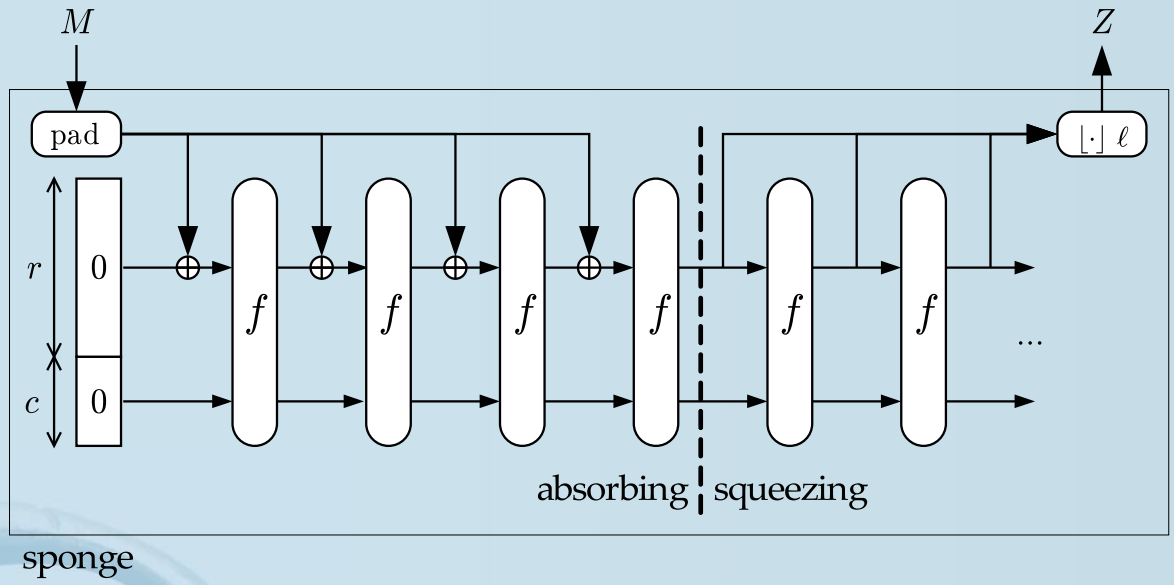
JH more rounds



JH features

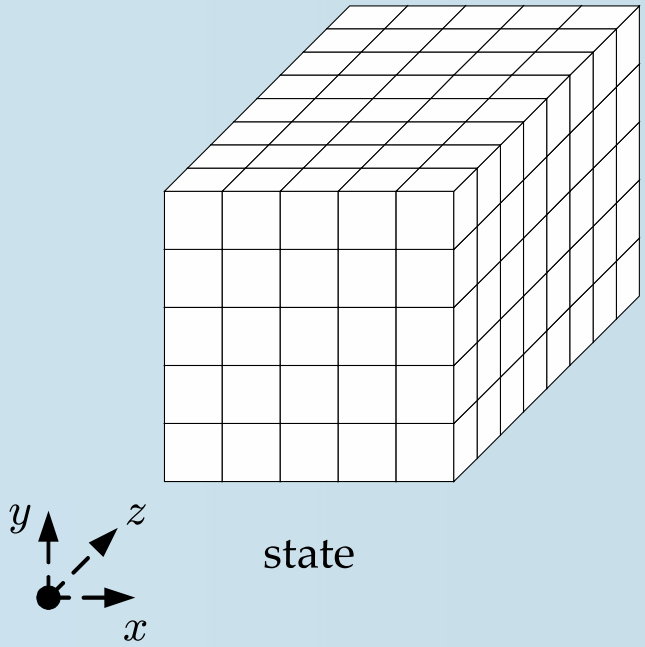
- “ShiftRows” different from AES
  - ~~Bounds on characteristics~~
- Comparatively low speed
- Rebound attack on full function (42 rounds)
  - Distinguisher

Keccak



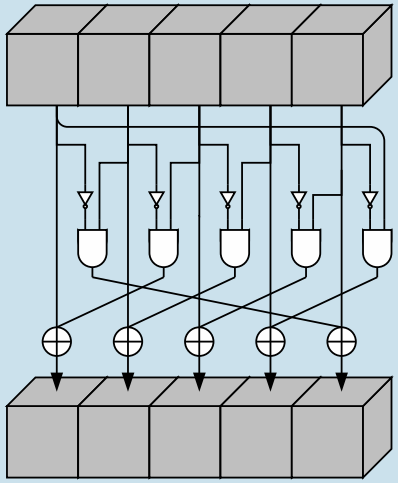
- Sponge
- 24 rounds

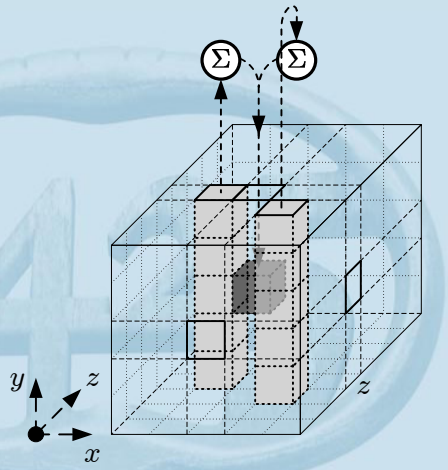
Keccak state

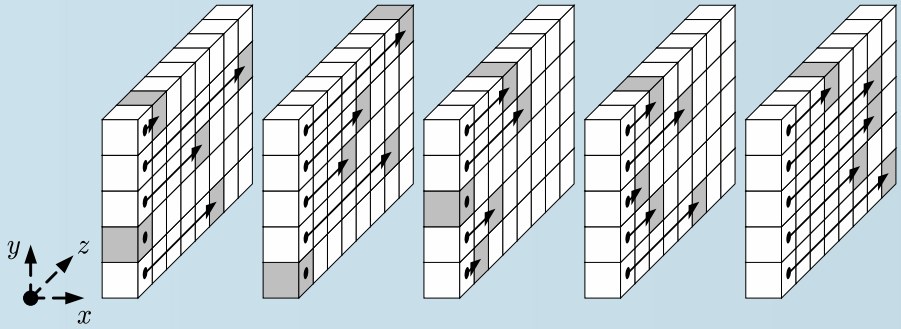


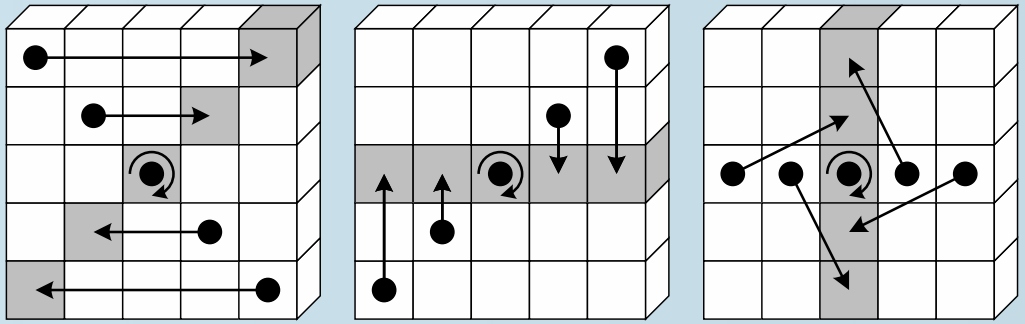
5 x 5 x 2/4/…/64 bit

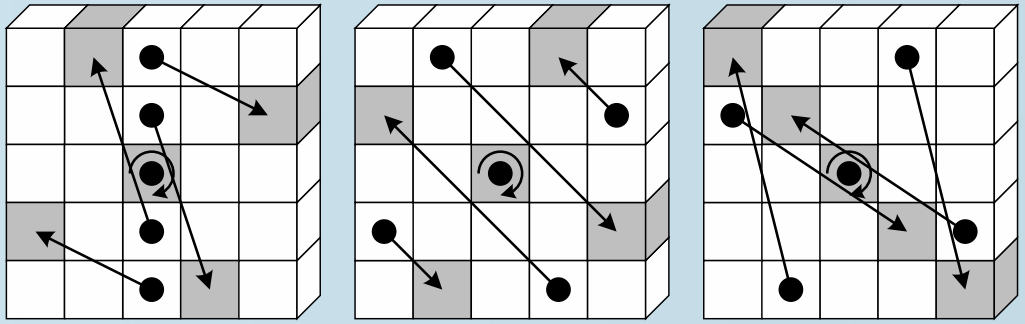
Keccak round steps









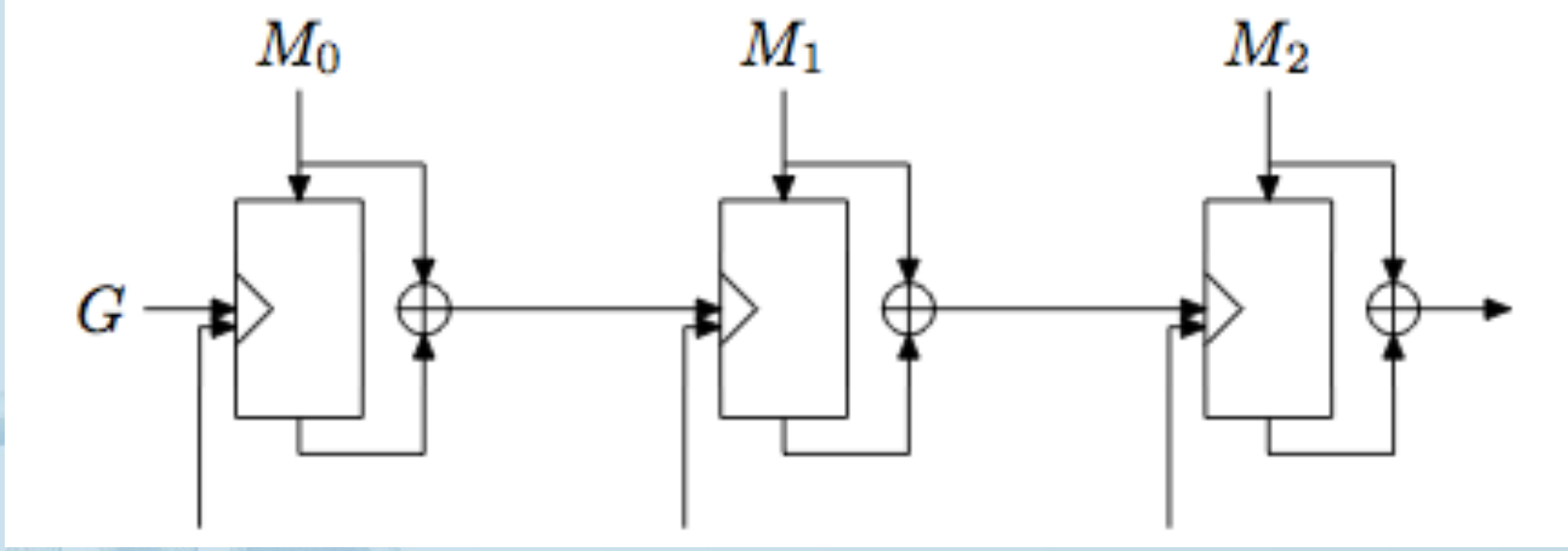


Keccak features

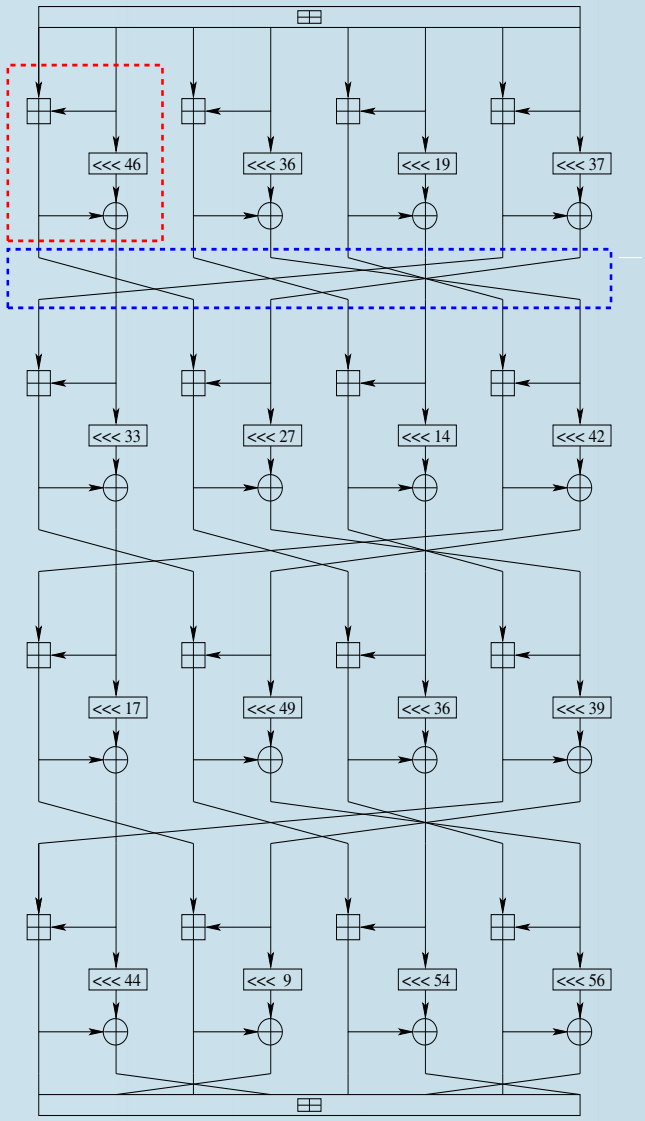
- Sponge: permutation-based
- Resembles 3D Cellular Automata
- Speed: in the middle

Skein: Unique Block Iteration (UBI)

- Mode of operation for a tweakable block cipher



Skein: Threefish



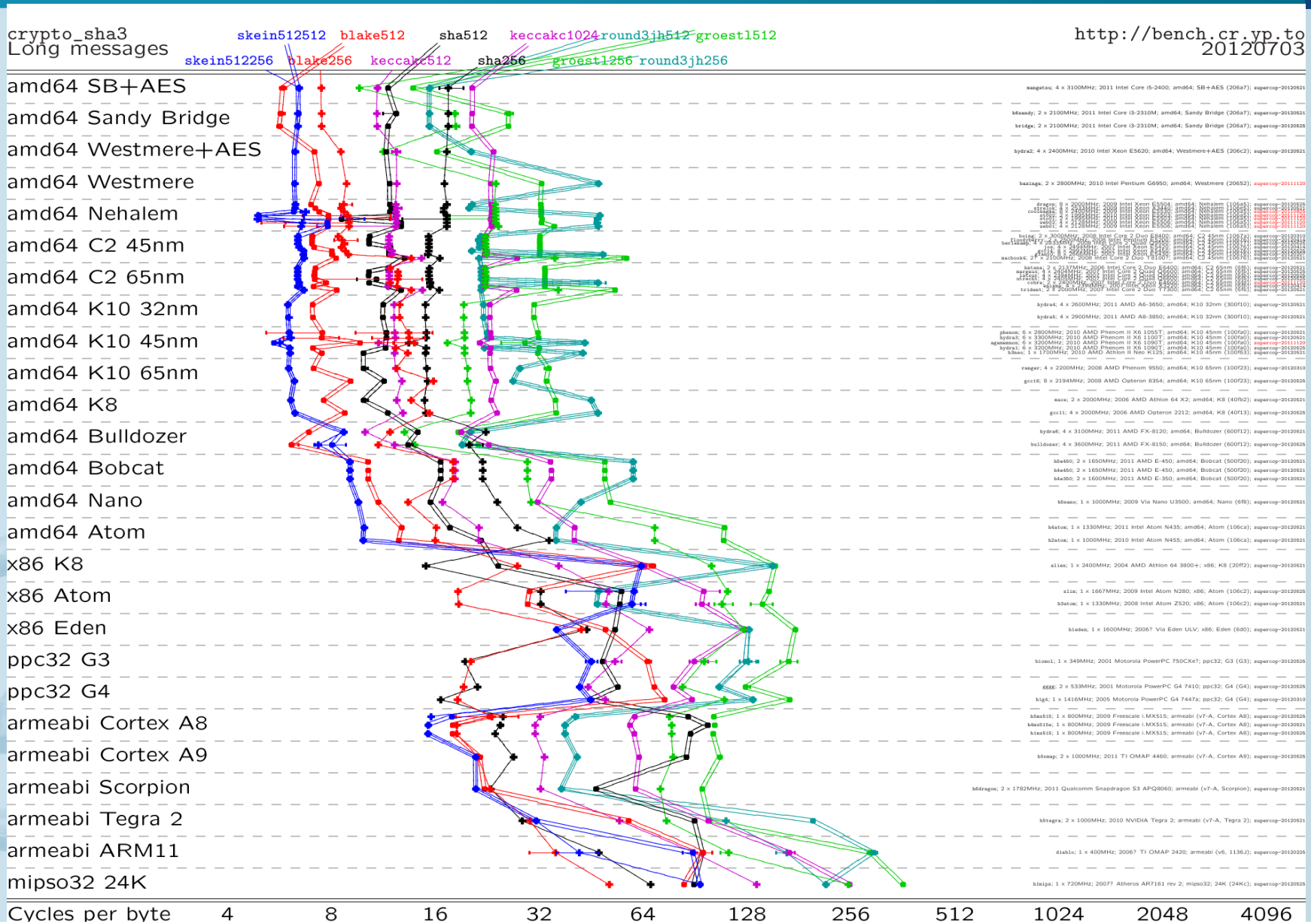
72 rounds

Skein features

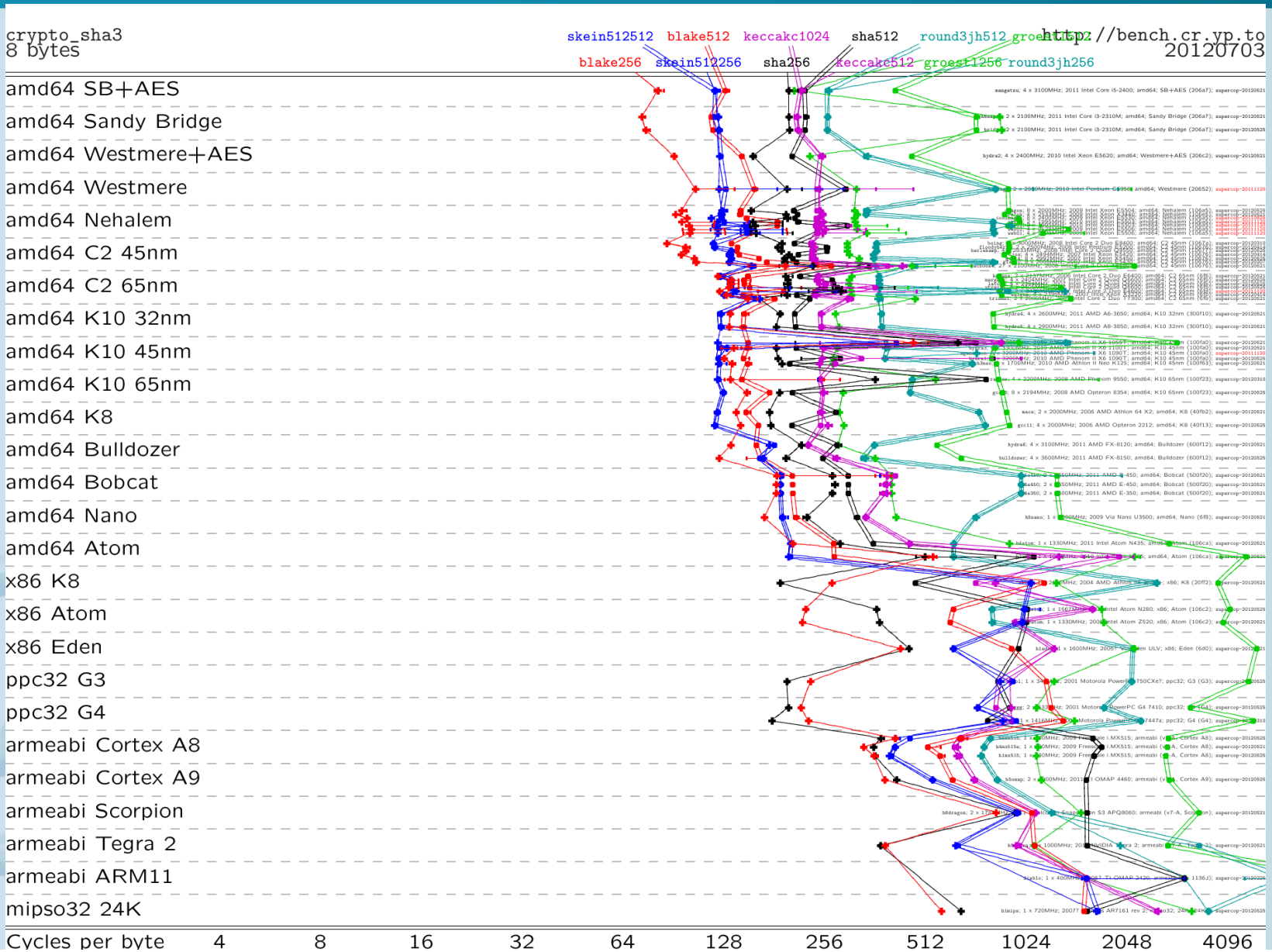
- ARX
- Very many rounds and fast
- Threefish is very different from Blowfish, Twofish

Speed

eBASH figures (long messages)



eBASH figures (short messages)

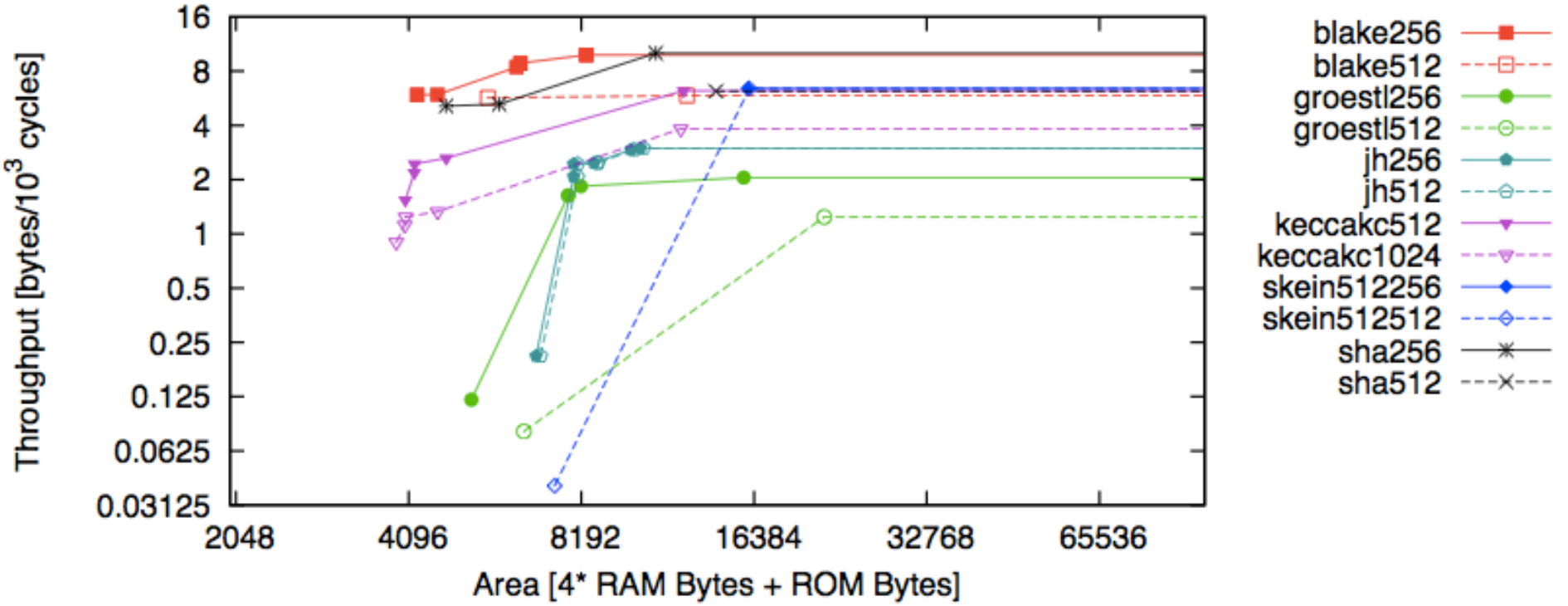


eBASH speed conclusions

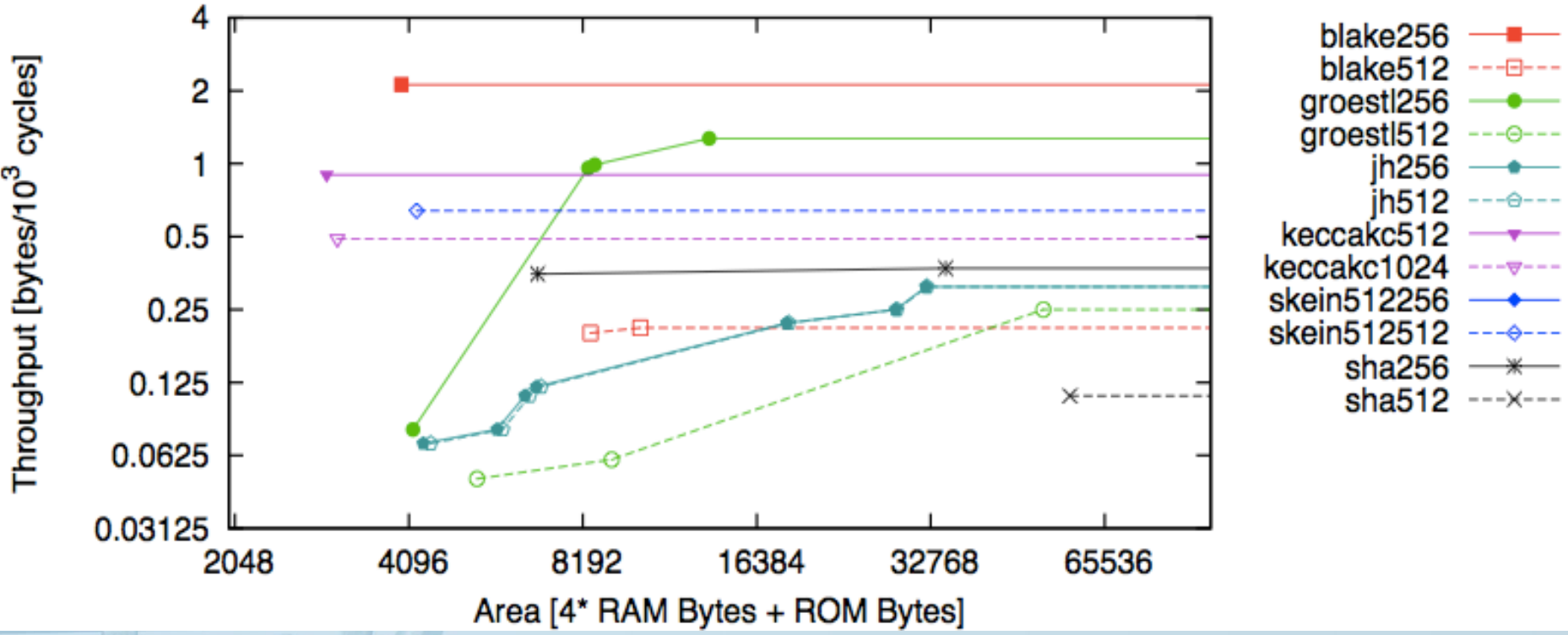
- Skein and BLAKE are the fastest
- Grøstl and JH are the slowest
- Keccak and SHA-256 in the middle

- ARX trumps S-boxes
  - Even with AES instruction extensions

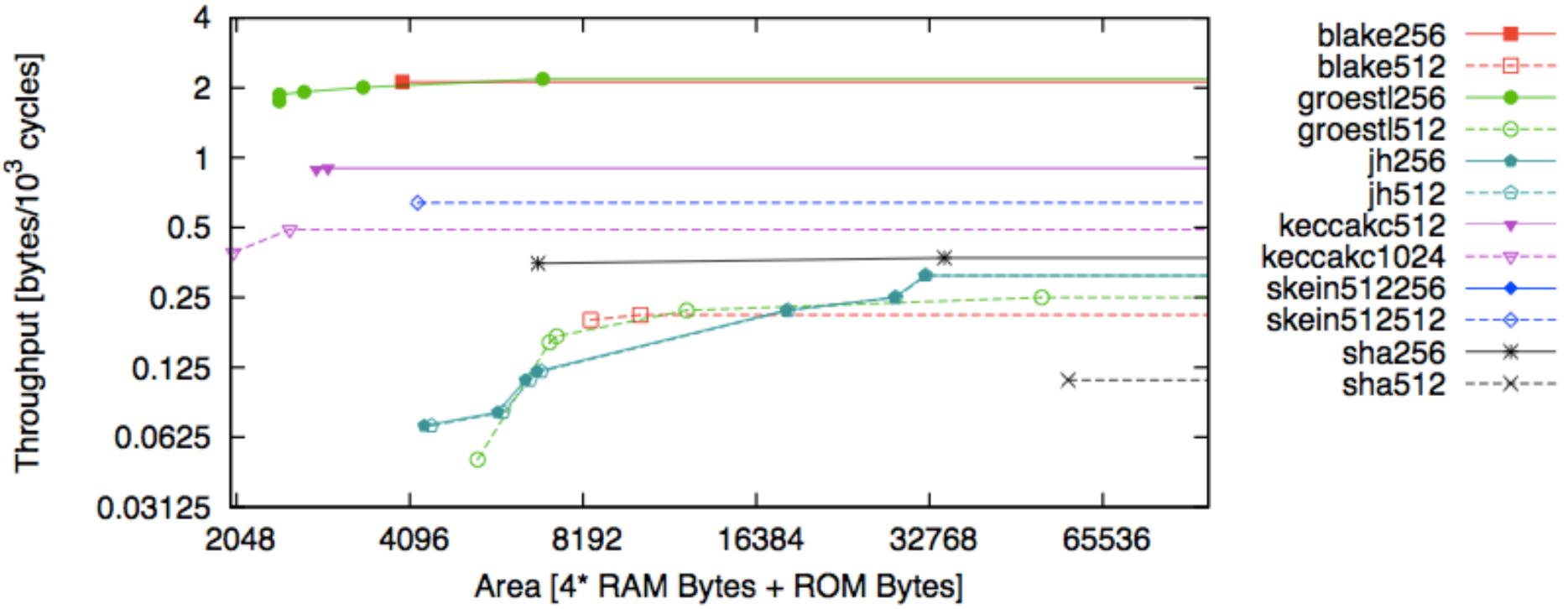
XBX figures: AR7 (32-bit)



XBX figures: ATmega1284P (8-bit)



XBX after Grøstl team intervention



XBX figures conclusions

- Minimum required area can be more important than speed
- BLAKE always among the best
  - Skein is the best on high-end platforms
- Keccak and Grøstl repeatedly among the best

- Figures depend greatly on effort spent

Minimal Sizes

256-bit	State size (+FF)	Message block	Rounds
BLAKE	512 (+ 1024)	512	14 (x2)
Grøstl	1024 (+512)	512	10
Keccak	1600	1088	24

512-bit	State size (+FF)	Message block	Rounds
BLAKE	1024 (+ 1024)	1024	16 (x2)
Grøstl	2048 (+1024)	1024	14
JH	1024 (+512)	512	42
Keccak	1600	576	24
Skein	512 (+1024)	512	72

SHA-3 key words

- Rebound
- Attack complexity/practicality
- Distinguisher – nonrandom property
- Provable security – indifferentiability

Remember the AES Key words?

- Security-margin weighted performance
- Side-channel attack resistance
- Algebra
- Pronunciation of Dutch vowels

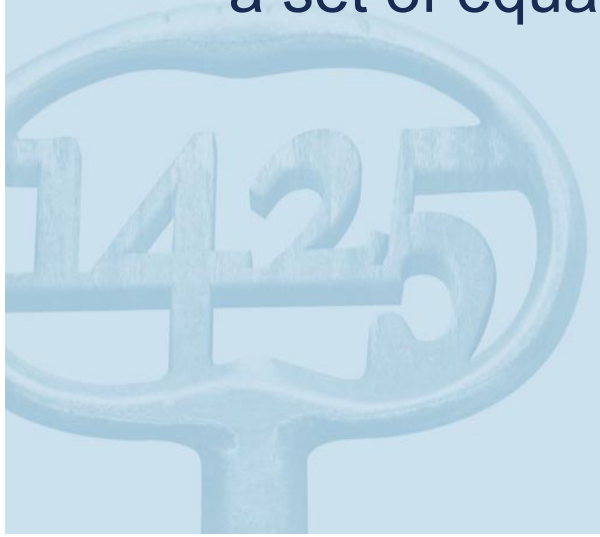
Rebound attack

- Differential cryptanalysis on hash functions
  - Look for characteristic ending in difference 0:

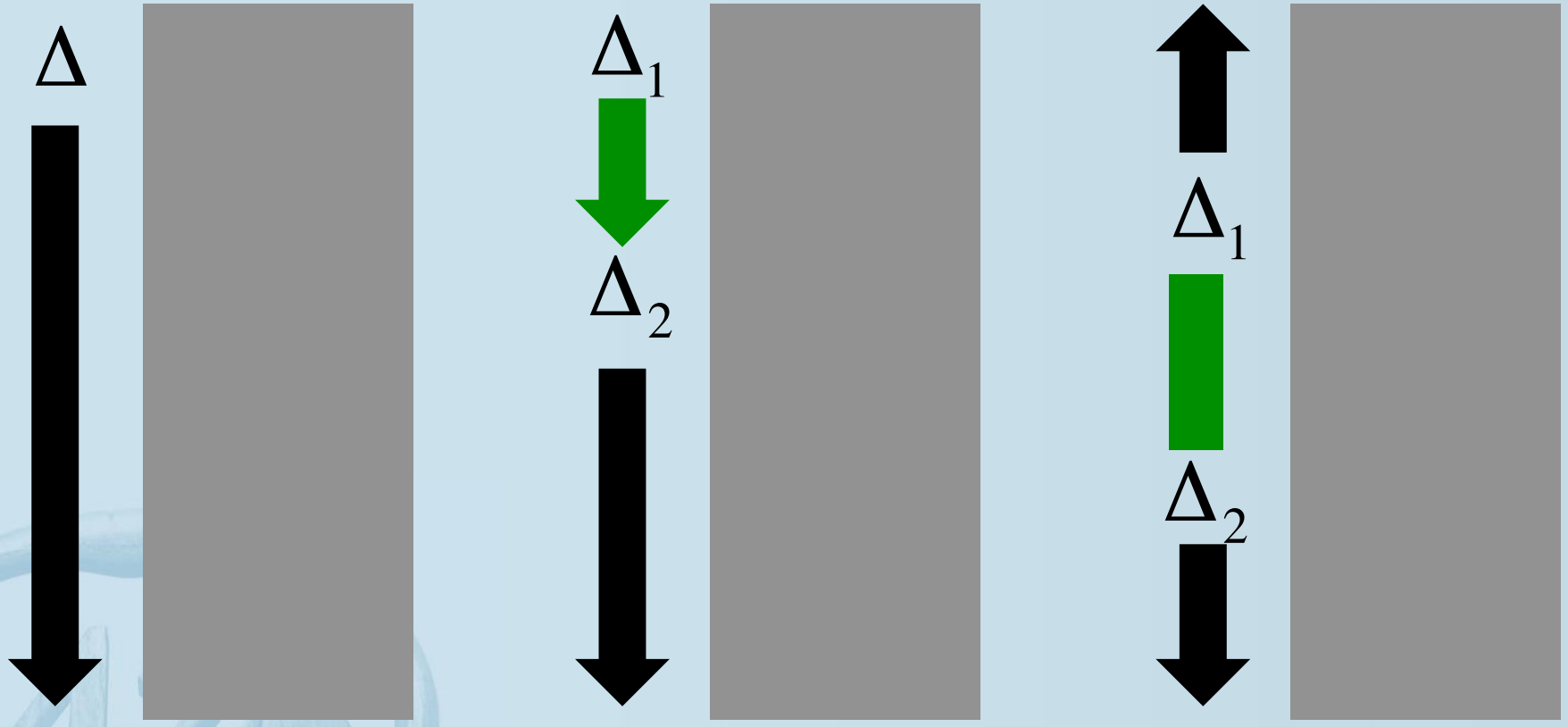
$$h(x \oplus \Delta) \oplus h(x) = 0 \Leftrightarrow h(x \oplus \Delta) = h(x)$$

  - Every right pair is a collision

- Finding right pairs: since there is no secret key, solving a set of equations deterministically (in principle)



Solving strategies



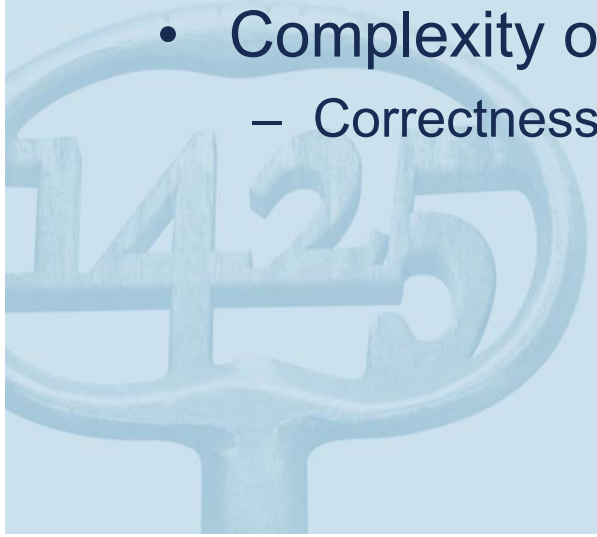
Classical

Message Modification

Meet-i-t-middle /rebound

Attack complexity

- How practical is attack X?
- Number of computations
  - Measured in equivalent hash computations?
- Amount of memory
  - Large memories are slow!
- Complexity of the description
  - Correctness!



Cube distinguishers

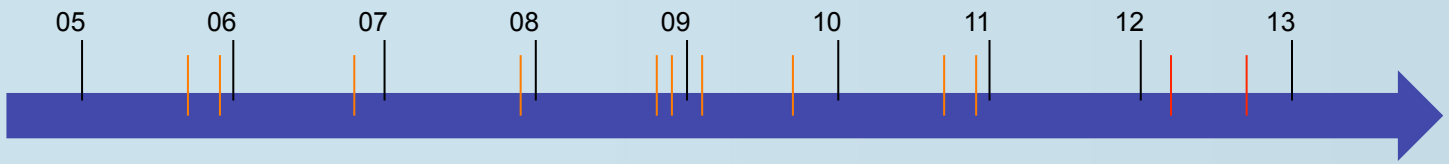
- Cube/AIDA/higher order differential: cube tester c

$$c(x) = \sum_{x \in V} f(x)$$

- Look for "special" c:
  - Equal to zero, linear, unbalanced, …

Cowboy sharpshooter

Timeline



Mar 2012: 3rd SHA-3 candidate conference

Oct 2012: Decision

Outcomes of the SHA-3 competition

- A winner: Keccak
  - Or SHA-256?
- Progress in knowledge on hash functions
  - And on AES security
- Semi-automatic tools and libraries
  http://www.ecrypt.eu.org/tools/